CLAIMS

1. An encryption method, comprising the steps of:

dividing a plaintext to be encrypted into a plurality of divided plaintexts; and

generating a product-sum type ciphertext constituted on a finite field by using the divided plaintexts and public keys.

2. The encryption method of Claim 1, wherein

said divided plaintexts are encoded, whereby each term of the intermediate decrypted text is constituted of an error correcting code word.

3. The encryption method of Claim 1, wherein:

a plurality of public keys are previously prepared for each of the divided plaintexts; and for each divided plaintext, an arbitrary public key is selected from among the prepared plurality of public keys, whereby a ciphertext is generated by using the selected public keys.

4. The encryption method of Claim 3, wherein

the public key is fixed for a predetermined number of divided plaintexts.

5. The encryption method of Claim 4, wherein

the predetermined number is one or two.

6. The encryption method of Claim 3, wherein

a ciphertext is generated such that selection information for indicating the public key selected for one divided plaintext is involved in another divided plaintext apart from the divided plaintext by a predetermined number.

7. The encryption method of Claim 6, wherein

the predetermined number is one or two.

8. A decryption method of decrypting a product-sum type ciphertext generated in accordance with the encryption method of Claim 1, wherein the decryption of divided plaintexts is performed sequentially starting from the lowest order term of the divided plaintexts of the ciphertext in ascending order.

9. A decryption method of decrypting a product-sum type ciphertext generated in accordance with the encryption method of Claim 1, wherein the decryption of divided plaintexts is performed sequentially starting from the highest order term of the divided plaintexts of the ciphertext in descending order.

10. A decryption method of decrypting a product-sum type ciphertext generated in accordance with the encryption method of

Claim 6, wherein the decryption process of a divided plaintext and the decryption process of selection information are carried out in parallel.

11. A cryptographic communication method for communicating information between a first entity and a second entity by using a ciphertext, comprising the steps of:

at the first entity, dividing a plaintext to be encrypted into a plurality of divided plaintexts;

at the first entity, generating a product-sum type ciphertext constituted on a finite field by using the divided plaintexts and public keys;

at the first entity, transmitting the generated ciphertext to the second entity; and

at the second entity, decrypting the transmitted ciphertext into a plaintext.

12. A cryptographic communication system for communicating information between plurality of entities by using a ciphertext, comprising:

an encryptor for generating a ciphertext from a plaintext in accordance with the encryption method of Claim 1;

a communication channel for transmitting the generated ciphertext from one entity to another entity; and

a decryptor for decrypting the transmitted ciphertext into a

plaintext.

13. A computer memory product having computer readable program code means for causing a computer to generate a ciphertext, said computer readable program code means comprising:

program code means for causing the computer to divide a plaintext to be encrypted into a plurality of divided plaintexts; and

program code means for causing the computer to generate a product-sum type ciphertext constituted on a finite field by using the divided plaintexts and public keys.

14. A computer data signal embodied in a carrier wave for transmitting a program, the program being configured to cause a computer to generate a ciphertext, comprising:

a code segment for causing the computer to divide a plaintext to be encrypted into a plurality of divided plaintexts; and

a code segment for causing the computer to generate a product-sum type ciphertext constituted on a finite field by using the divided plaintexts and public keys.